The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
10/26/2011

SUBJECT: Microsoft Outlook Web Access Session Replay Security Bypass Vulnerability

OVERVIEW:
A security bypass vulnerability has been discovered in Microsoft Outlook Web Access (OWA). Microsoft OWA is a browser-based application that is used to access email, calendars, contacts, tasks, documents, and other Outlook mailbox content remotely. This vulnerability will allow an attacker to login to Outlook user accounts without supplying the user's authentication credentials. Successful exploitation will result in an attacker gaining unrestricted access to the user's OWA account. The attacker could then send, view, change, or delete user data such as email, calendar appointments, or tasks, or create auto-forward rules that may allow an attacker to obtain copies of the emails.

SYSTEMS AFFECTED:

- Microsoft Outlook Web Access 8.2.254.0 (Microsoft Exchange 2007)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: High

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:
A new security bypass vulnerability has been discovered in Microsoft Outlook Web Access (OWA). This vulnerability will allow an attacker to access Outlook user accounts without supplying the user's authentication credentials. This is done by an attacker monitoring network traffic for a successful authentication session with the Exchange server. The attacker then replays the web request using the captured cookie to clone a user's browser session. Please note that this vulnerability only affects OWA associated with Exchange 2007. The most likely attack vector is a man-in-the-middle attack over a Local Area Network (LAN).

Currently, there is no patch available for this vulnerability. Successful exploitation will result in an attacker gaining unrestricted access to the user's OWA account. The attacker could then send, view, change, or delete user data such as email, calendar appointments, or tasks, or create auto-forward rules that may allow an attacker to get copies of the emails.

RECOMMENDATIONS:

The following actions should be taken:

- Consider restricting OWA access to trusted networks.
- If there is no business need, consider disabling OWA capabilities.
- Consider upgrading to Exchange 2010.
- Implement a Virtual Private Network (VPN) for remote users.

REFERENCES:

Security Focus:

http://www.securityfocus.com/bid/50361

Full Disclosure:

http://seclists.org/fulldisclosure/2011/Oct/818